Remarks

Reconsideration is requested in view of the preceding amendments and the following remarks.

New claims 29-30 are submitted for consideration. Support for new claims 29-30 can be found in the specification at, for example, Table 1. No new matter is introduced.

Claims 1-3, 5-8, 11-13, and 15-16 stand rejected as allegedly being directed to non-statutory subject matter. The rejection of claims 1-3, 11-13, and 15-16 is moot in view of the cancellation of these claims without prejudice. The rejection of claims 5-8 is traversed. Claims 5-8 recite methods for obtaining a Montgomery product of a first cryptographic parameter and a second cryptographic parameter. Cryptographic parameters are associated with physical activity, i.e., secure communication between a message sender and a message recipient. These methods do not merely manipulate an abstract idea or perform a purely mathematical algorithm. Instead, the claimed methods apply a particular Montgomery multiplication method to produce a useful, concrete, and tangible result. The practical significance of such manipulation of cryptographic parameters is amply evidenced by the art cited by the Patent Office and the applicants. For example, according to Monier, U.S. Patent 5,745,398, cryptographic applications of Montgomery multiplication methods can be found in message authentication, user identification, and key exchange. Withdrawal of this rejection is requested.

Claim 5 stands rejected as allegedly anticipated by Monier, U.S. Patent 5,745,398 ("Monier"). This rejection is traversed. Claim 5 as amended recites a method for obtaining a Montgomery product of a first cryptographic parameter X and a second cryptographic parameter Y with respect to a modulus M, wherein X and Y are represented by m bits. The method includes selecting a word length w and a number of words e, and representing the second cryptographic parameter and the modulus M as e words of length w, wherein e is at least 2. An intermediate value of a first word of the Montgomery product is obtained based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter.

According to the Office action, Monier discloses such a method at col. 3, lines 38-54 and col. 4, lines 1-28. This is incorrect. Monier fails to teach or suggest obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter and a bit of the first cryptographic parameter. According to Monier, an

intermediate data element is produced by supplying m words of a parameter $H = 2^{(a+b)k} \bmod N$ and a words of a multiplicand A to a multiplication circuit, wherein a and b are numbers of k bit word representing a multiplicand A and a multiplier B, respectively. Such an intermediate data element value is not a intermediate value of a Montgomery product based on based a product of a words of the second cryptographic parameter and a bit of the first cryptographic parameter as recited in claim 5. For at least this reason, claim 5 and dependent claims 4, 6-10, and 26-29 are properly allowable over Monier.

Dependent claims 6-10 and 29 recite additional features that are neither taught nor suggested by Monier. For example, claim 7 recites obtaining an intermediate value of a second word of the Montgomery product based on a product of a second word of the second cryptographic parameter and a second bit of the first cryptographic parameter in parallel with obtaining the intermediate value of the first word. Monier does not teach or suggest obtaining intermediate values of first and second words of a Montgomery product in parallel. The cited portion of Monier merely teaches a parallel input that can receive words. Claim 8 recites updating the intermediate value of the first word of the Montgomery product with a contribution from at least one product of a second selected bit of the first cryptographic parameter-with at least a second selected word of the second cryptographic parameter. Monier does not teach or suggest updating an intermediate value in this way. New claim 29 recites obtaining an intermediate value of a first word of the Montgomery product based on a product of a word of the second cryptographic parameter, a word of the modulus, and a bit of the first cryptographic parameter. Monier does not teach or suggest obtaining an intermediate value of a Montgomery product in this way. For at least these reasons, claims 7, 8, and 29 are properly allowable over Monier.

Claim 17 recites an apparatus for performing a Montgomery multiplication of a first operand and a second operand with respect to a modulus. The apparatus comprises a plurality of processing elements that include inputs for words of the first operand, words of the modulus, an intermediate value of a word of a Montgomery product, and an input for a bit of the second operand. A control unit is situated and configured to direct words of the first operand, words of the modulus, and bits of the second operand to the processing elements. Monier does not teach or suggest such apparatus. Monier's Fig. 1 illustrates an integrated circuit configured to receive a multiplicand A, a multiplier B, and a modulus N as serial data at respective serial inputs A_{i-1}, B,

and N in communication with respective MUXes 24, 13, 15. Monier's Fig. 1 circuit is not configured to receive words of the first operand, the modulus, and the intermediate value. Monier's multiplication circuits also fail to include the word inputs recited in claim 17. Monier's multiplication circuits 19, 20 each have a serial input, a parallel input, and a serial output, i.e., these circuits each have at most one word input, and do not have the word inputs recited in claim 17. The only word (parallel) inputs in Monier's Fig. 1 are associated with supplying words of A_{i-1} to multiplier 19, words of a correction value J_0 to multiplier 20, and words of a product $X_0(i)*J_0$ mod 2 to the multiplier 20. Monier lacks any teaching or suggestion of a plurality of processing elements having word inputs for the first operand, the modulus, and an intermediate value. For at least this reason, claim 17 and dependent claims 18-19 and 25 are allowable over Monier.

Claim 20 recites a circuit for obtaining a Montgomery product of first and second operands with respect to a modulus. The circuit includes, in part, at least a first processing element and a second processing element, each of the processing elements including inputs that receive words of the first operand and the modulus, and outputs that deliver values of words of the Montgomery product. Monier does not teach or suggest such a circuit. Monier's Fig. 1 does not include any input configured to receive words of the modulus, and has only a single input configured to receive words of the first operand -- the input associated with the multiplier circuit (19). Thus, Monier's Fig. 1 circuit does not include the inputs recited in claim 20. For at least this reason, claim 20 and dependent claims 21-22 are properly allowable.

Claim 23 recites a task processor for obtaining a Montgomery product of a first operand and a second operand with respect to a modulus M. The task processor comprises, in part, an input configured to receive a bit of the first operand, an input configured to receive a word of the second operand, and an input configured to receive a word of the modulus. As noted above, Monier does not teach or suggest an input configured to receive a word of the modulus. Claim 23 also recites an output configured to supply a final or intermediate value of a word of the Montgomery product. Monier also fails to teach or suggest such an output. Instead, Monier discloses only a serial output. See Monier, Fig. 1 and col. 3, line 49. For at least these reasons, claim 23 and dependent claim 24 are properly allowable over Monier.

New claim 30 recites a smart card comprising a Montgomery multiplication module having a word input configured to receive words of a first cryptographic parameter, a word input

configured to receive words of a modulus, and a bit input configured to receive bits of a second cryptographic parameter. As noted above, Monier does not teach or suggest a word input configured to receive words of a modulus. For at least this reason, claim 30 is properly allowable over Monier.

All pending claims are in condition for allowance, and action to such end is respectfully requested.

Respectfully submitted,

KLARQUIST SPARKMAN, LLP

By _____
Michael D. Jones
Registration No. 41,879

One World Trade Center, Suite 1600
121 S.W. Salmon Street
Portland, Oregon 97204
Telephone: (503) 595-5300
Facsimile: (503) 228-9446